



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|--------------------------|------------------|
| 09/767,128 | 01/22/2001 | Radia J. Perlman | P4098 | 2127 |
| 207 | 7590 | 11/07/2003 | EXAMINER | |
| WEINGARTEN, SCHURGIN, GAGNEBIN & LEOVICI LLP TEN POST OFFICE SQUARE BOSTON, MA 02109 | | | CHEUNG, MARY DA ZHI WANG | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 3621 | |

DATE MAILED: 11/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/767,128

Applicant(s)

PERLMAN, RADIA J.

Examiner

Mary Cheung

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 August 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) 12-16 and 21-27 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11, 17-20 and 28-37 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2,3.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Status of the Claims

1. This action is in response to the communication filed on August 13, 2003. Claims 1-37 are pending. On July 23, 2003, an office action of Election/Restriction mailed to the applicant. Examiner grouped the pending claims into two groups. Group I includes claims 1-10, 17-20 and 28-37. Group II includes claims 12-16 and 21-27. Applicant has elected groups I (claims 1-10, 17-20 and 28-37) in the response filed on August 13, 2003. Examiner noticed that claim 12 is omitted from the Election/Restriction, and contacted attorney Victor Lebovici on October 21, 2003 to discuss this matter. Per phone conversion, attorney Victor Lebovici agreed to elects Group I, which includes claims 1-11, 17-20 and 28-37, without traverse. Thus the status of the claims as following:

Claims 1-37 are pending. Claims 1-11, 17-20 and 28-37 have been elected without traverse. Claims 12-16 and 21-27 are withdrawn from consideration.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 33 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 33 recites the limitation "said program code for publishing said certificate" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 4-5, 7-9, 11, 17-18, 20, 34 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320.

As to claim 1, de Silva teaches a method for certificate generation comprising the steps of (abstract):

- a) Forwarding a request from a first node to a second node to generate a certificate, wherein said request includes a first identifier that identifies the first node (column 4 lines 41-44 and column 12 lines 12-15 and Figs. 6-8);
- b) In response to receipt of the request at the second node, generating a certificate (column 4 lines 44-58 and column 12 lines 15-19 and Figs. 6-8).

De Silva does not explicitly state that the certificate is generated further includes said first identifier. However, de Silva specifically states that due to the sensitive nature of digital certificate services, all communications preferably occur over secure communication links (column 11 lines 30-44 and column 12 lines 47-50). It would have been obvious to one of ordinary skill in the art to allow the certificate in de Silva's teachings to include the identifier of the first node because this would allow the system more securely monitoring the generated certificates.

As to claim 4, de Silva teaches authenticating said certificate by said second node (column 4 lines 55-67).

As to claim 5, de Silva teaches authenticating said certificate comprises the step of generating a certificate digitally signed by said second node (column 1 lines 48-50 and column 11 lines 34-44).

As to claim 7, de Silva teaches the certificate includes a time stamp that identifies expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that identifies a time associated with the request. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva's certificate to include a time associated with the request because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 8, de Silva teaches authenticating said request by said first node (column 4 lines 41-53).

As to claim 9, de Silva does not explicitly digitally signing said request by said first node. However, de Silva specifically teaches digitally signing the certificate against subsequent tampering (column 1 lines 48-50). It would have been obvious to one of ordinary skill in the art to allow the certificate in de Silva's teachings to be signed by the first node for preventing unauthorized access of the certificate.

As to claim 11, de Silva teaches the certificate includes a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that is associated with a time and

Art Unit: 3621

date when said request was received by said second node. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva's certificate to include a time and date associated with said request was received by the second node because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 37, de Silva further teaches revoking untrustworthy certificates (column 1 lines 11-15, 55-58 and column 4 line 65 – column 5 line 10).

Claims 17-18, 20, 34 and 36 are rejected for the similar reasons as claims 1, 4 and 11.

6. Claims 2-3, 6, 10, 19, 28-33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Vaeth et al., U. S. Patent 6,308,277.

As to claim 2, de Silva teaches said request further includes information related to the principal that requesting a certificate (column 12 lines 1-14). De Silva does not specifically state that the information further includes a second identifier that identifies the principal. However, Vaeth teaches this matter (column 4 lines 34-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the request information in de Silva's teachings to include a second identifier that identifies the principal because this would allow the system more securely monitoring transactions among the different terminals for better protecting the secrecy of each transaction.

As to claim 3, the modified method of de Silva teaches generating a certificate as discussed above. De Silva does not specifically teach said certificate further includes a public key associated with said principal, and said second identifier. However, Vaeth teaches this matter (column 4 lines 34-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow said certificate in de Silva's teachings further includes a public key associated with said principal, and said second identifier because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 6, de Silva teaches generating a certificate digitally signed by said second node as discussed above. De Silva does not specifically teach generating a certificate digitally signed by said second node using a private key of a public private key pair associated with said second node. However, Vaeth teaches this matter (column 4 lines 34-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in de Silva's teachings to be signed by using a private key of a public private key pair associated with said second node because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 10, the modified by method of de Silva teaches the certificate is digitally signed as discussed above. De Silva does not specifically teach the certificate is digitally signed by using a private key of a public/private key pair associated with said first node. However, Vaeth teaches this matter (column 4 lines 34-61). It would have

Art Unit: 3621

been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in de Silva's teachings to be signed by using a private key of a public/private key pair associated with said first node because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 28, de Silva teaches a computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for generating a certificate, said computer program being executable by a processor and comprising (abstract);

- a) Program code for receiving a request from a registration authority to issue a certificate behalf of a principal (column 4 lines 34-53 and column 12 lines 6-15 and Figs. 6-8);
- b) Program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority (column 4 lines 44-58 and column 12 lines 14-19 and Figs. 6-8).

De Silva does not explicitly state that said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority. However, Vaeth teaches this matter (column 4 lines 34-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in de Silva's teachings to include the

identifiers as described hereinabove because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 29, de Silva teaches the program code for generating said certificate is further operative to include within said certificate a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that is associated with a time of receipt by said certification authority of said request from said registration authority of said request to issue said certificate. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva's certificate to include a time stamp that is associated with a time of receipt by said certification authority of said request from said registration authority of said request to issue said certificate because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 32, de Silva teaches the computer program code includes program code for publishing said certificate (column 4 lines 57-58).

As to claim 33, de Silva teaches the program code for publishing said certificate includes program code for forwarding said certificate to a directory server (column 12 lines 14-19).

Claims 19 and 35 are rejected for the similar reasons as claims 2-3.

Claims 30-31 are rejected for the similar reasons as claims 28-29.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Brickell et al. (U. S. Patent 5,867,578) discloses a multi-step digital signature system and method is provided having a distributed root certifying authority.

Andrews et al. (U. S. Patent 6,324,645) discloses a public key management infrastructure is shared by at least two users.

Bisbee et al. (U. S. Patent 6,367,013) discloses digital signature chaining.

Patel et al. (U. S. Patent 6,438,690) discloses a secure end-to-end communications system includes a vault controller based registration application for managing the issuance and administration of digital certificates for use in conducting electronic commerce in the system.

Okumura et al. (U. S. Patent 6,553,493) discloses assigning a key pair to an entity such as a certification authority.

Aull (EP 1 162 781 A2) discloses generation of signature certificate in a Public Key Infrastructure that includes sending a new user a first piece of information required for generation of a signature certificate for the new user.

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is (703)-305-0084. The examiner can normally be reached on Monday – Thursday from 8:00 AM to 5:30 PM. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell, can be reached on (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

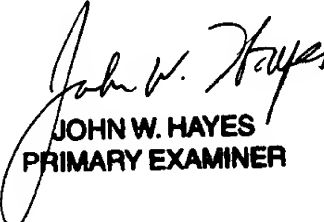
The fax phone number for the organization where this application or proceedings is assigned are as follows:

(703) 872-9306 (Official Communications; including After Final
Communications labeled "BOX AF")

(703) 746-5619 (Draft Communications)

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, 7th Floor Receptionist.

Mary Cheung
Patent Examiner
Art Unit 3621
October 30, 2003


JOHN W. HAYES
PRIMARY EXAMINER